UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

JULIO LOPEZ and MICHAEL OROS, *On Behalf of Themselves and All Others Similarly Situated*, Plaintiffs, v. VOLUSION, LLC, Defendant.	Cause No. 1:20-cv-00761 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Julio Lopez and Michael Oros (collectively, "Plaintiffs"), individually and on behalf of all other persons similarly situated, and through their attorneys of record, allege the following against Defendant Volusion, LLC ("Defendant" or "Volusion") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Volusion is a technology company which provides "the infrastructure behind some of the most successful ecommerce stores online."[1] It offers an "all-in-one platform" for businesses to set up e-commerce shops, including by offering services that allow business to accept credit card payments.[2] Volusion provides its services to thousands of e-commerce stores.[3]

2. Between on or about September 7, 2019 and October 10, 2019, unauthorized third parties were able to steal consumers' personally identifiable information ("PII") from Volusion's e-

[1] https://www.volusion.com/company.
[2] https://www.volusion.com/all-features.
[3] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/.

commerce platform by inserting malicious code into a Volusion JavaScript library; while much of the code appeared legitimate, it included a "payment card skimmer."[4] Independent researchers determined that up to 6,589 online stores were connected to the compromised Volusion domain hosting the JavaScript library.[5]

3. Consumers who made purchases through the online stores using Volusion's compromised payment software during this time period had their card details and other personal information stolen and passed to an unauthorized third party (herein, the "Data Breach").[6] According to Volusion, the PII stolen in the Data Breach "may have included names, addresses, phone numbers, email addresses, credit card numbers, CVVs, and expiration dates."[7]

4. On October 9, 2019, Trend Micro's Security Intelligence Blog reported that it had discovered an "online credit card skimming attack" that was "actively operating on 3,126 online shops" hosted on Volusion's e-commerce platform.[8]

5. By March 12, 2020, the Gemini Advisory firm identified over 239,000 compromised credit card records from the Data Breach that were sold on the dark web for $1.6 million. Gemini estimates that, based on the number of affected merchants, the total number of compromised financial records could be as high as 20 million. At the same cost for which the original set of 239,000 stolen records were sold, the haul could net the hackers as much as $133.89 million on the dark web.[9]

6. Yet it was not until April 21, 2020, that Volusion distributed a notice of the Data Breach to its victims, including Plaintiffs Lopez and Oros.

---

[4] *Id.; see also* https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.

[5] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/.

[6] *Id.*

[7] https://oag.ca.gov/system/files/US%20Notice%20Proof.pdf.

[8] https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.

[9] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/.

7. Plaintiffs and the Class had their PII stolen as a result of the Data Breach and suffered harm directly as a result of the Data Breach.

PARTIES

8. Mr. Lopez is a citizen of the state of Florida, and at all relevant times has resided in Miami, Florida. He provided PII to Pelindaba Lavender, a merchant hosted on the Volusion e-commerce platform, and Volusion when making a purchase on or about September 25, 2019. Mr. Lopez's PII was stolen in the Data Breach. Mr. Lopez received an email titled "Notice of Data Incident" from Volusion dated April 21, 2020, advising that his PII was stolen in the Data Breach.

9. Mr. Oros is a citizen of the state of Illinois, and at all relevant times has resided in Lee, Illinois. He provided PII to at least one online merchant using the Volusion e-commerce platform. Mr. Oros's PII was stolen in the Data Breach. Mr. Oros received an email titled "Notice of Data Incident" from Volusion dated April 22, 2020, advising that his PII was stolen in the Data Breach.

10. Defendant Volusion, LLC is a corporation incorporated in the State of Delaware with its headquarters and principal place of business in Austin, Texas. Volusion is majority owned (88.31%) by KSCO Holdings, Inc., a Texas entity. Volusion, LLC may be served through its registered agent: National Registered Agents, Inc., 1999 Bryan Street, Suite 900, Dallas, TX 75201.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members, including Plaintiffs, are citizens of a different state than Defendant.

12. This Court has personal jurisdiction over Volusion because it is authorized to and

regularly conducts business in Texas and is headquartered in Austin, Texas.

13. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Volusion Collected Consumers' PII

14. Volusion is a technology company which provides "the infrastructure behind some of the most successful ecommerce stores online." It offers an "all-in-one platform" for businesses to set up e-commerce shops, including by offering services that allow business to accept credit card payments. Volusion provides its services to thousands of e-commerce stores.

15. To purchase an item through an online shop hosted on Volusion's e-commerce platform, a consumer must enter the following PII: name, address, phone number, email address, credit card number, CVV, and expiration date. Volusion retains records of the PII of consumers who made purchases from online shops hosted on its e-commerce platform.

16. The PII provided to Volusion by consumers shopping on the Volusion e-commerce platform is governed by its merchant clients' privacy policies. Volusion makes available to its customers a "simple and FREE template to instantly generate a custom privacy policy for your business" (herein, the "Volusion Template Privacy Policy").[10]

17. The Volusion Template Privacy Policy provides information about what types of PII will be collected from consumers and how that data will be shared. It further promises the consumer that Volusion's merchant clients "take reasonable measures, including administrative, technical, and physical safeguards, to protect information about you from loss, theft, misuse, unauthorized access, disclosure, alteration, and destruction."[11]

[10] https://www.volusion.com/tools/privacy-policy-generator.
[11] *Id.*

18. The relationship between Volusion and its merchant clients is governed in part by Volusion's own privacy policy (the "Privacy Policy"). The Privacy Policy provides that Volusion "will take commercially reasonable precautions to protect the information from loss, misuse and unauthorized access, disclosure, alteration and destruction. We follow industry standards on information security management to safeguard sensitive information, and are certified as a PCI-DSS service provider. Our platform is audited annually by a third-party qualified security assessor for compliance with PCI-DSS."[12]

19. Mr. Lopez provided PII to Pelindaba Lavender, a merchant hosted on the Volusion e-commerce platform, and Volusion when making a purchase on or about September 25, 2019. In making this purchase, he entered his first name, last name, address, city, state, zip code, phone number, email address, and credit card information. It appears that Pelindaba Lavender displays an older version of the Volusion Template Privacy Policy, as it contains language identical to other Volusion stores, all of which have similar representations regarding data safety to the current Template Privacy Policy.[13]

20. Mr. Oros provided PII to one or more merchants using the Volusion e-commerce platform. According to the Notice of Data Incident Mr. Oros received from Volusion on or about April 22, 2020, the PII that was compromised included names, addresses, phone numbers, email addresses, credit card numbers, CVVs, and expiration dates, including the debit card associated with Mr. Oros's account.

21. Plaintiffs provided their PII to Volusion with the expectation and understanding that Volusion would adequately protect and store their data. If they had known that Volusion's data security was insufficient to protect their PII, they would not have entrusted their PII to Volusion (or

[12] https://www.volusion.com/privacy-policy.

[13] *Compare* https://www.pelindabalavender.com/terms_privacy.asp *with* http://store.heartlandnatural.com/terms_privacy.asp, https://www.dallasshowroomsales.com/terms_privacy.asp, and https://www.aglamesis.com/Articles.asp?ID=5.

its merchant clients), and would not have been willing to pay for, or pay as much for, the items they purchased from online stores hosted on the Volusion platform. In other words, they would not have used Volusion's payment processing software to make their purchases.

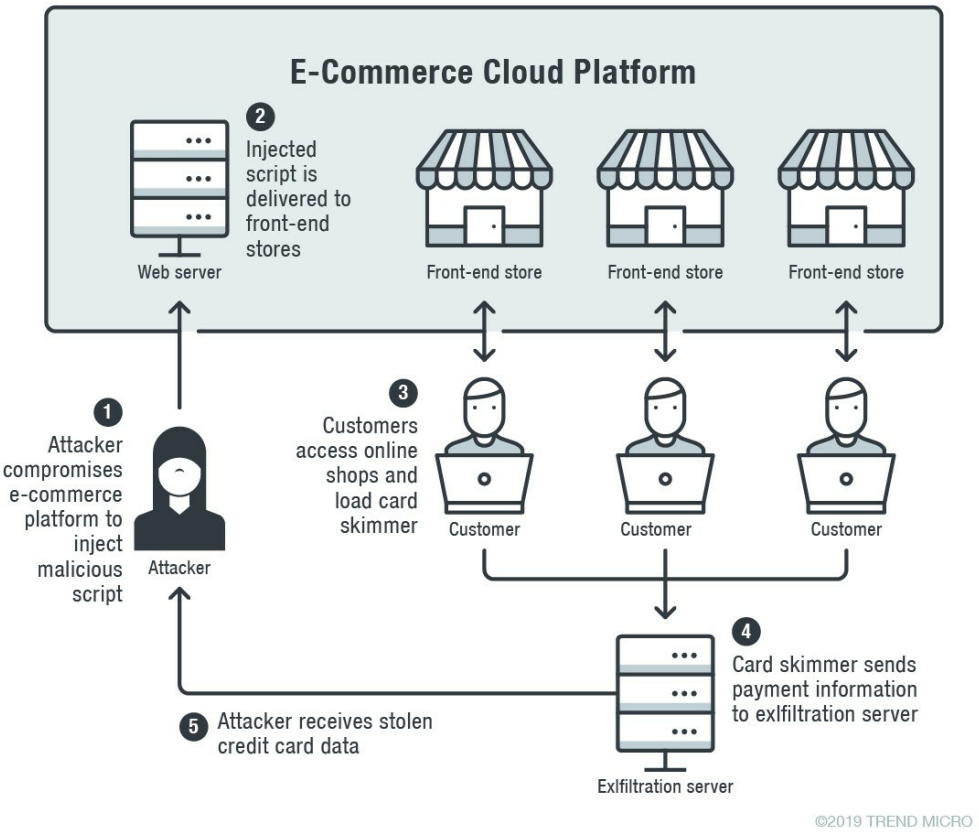
The Data Breach

22. On or about September 7, 2019, unauthorized third parties were able to insert malicious code into a Volusion JavaScript library due to Volusion's lax security measures; while much of the code appeared legitimate, it included a "payment card skimmer."[14] Independent researchers determined that up to 6,589 online stores, including stores such as the Sesame Street Live online store, were connected to the compromised Volusion domain hosting the JavaScript library.[15]

23. This method of obtaining authorized access to users' personal information is also referred to as a "web skimmer."

24. Once entered onto a webpage compromised by a web skimmer, users' PII is forwarded to an exfiltration server, where it may be used to create clone cards for fraudulent online purchases or sold in batch information dumps on underground forums. The following chart prepared by Trend Micro demonstrates how the process works:

[14] *Id.; see also* https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.
[15] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/; *see also* https://www.zdnet.com/article/hackers-breach-volusion-and-start-collecting-card-details-from-thousands-of-sites/.



25. Consumers who made purchases through online stores using Volusion's compromised payment software during this time period had their card details and other personal information stolen and passed to an unauthorized third party.[16] According to Volusion, the information stolen in the Data Breach "may have included names, addresses, phone numbers, email addresses, credit card numbers, CVVs, and expiration dates."[17]

26. On October 9, 2019, Trend Micro's Security Intelligence Blog reported that it had discovered an "online credit card skimming attack" that was "actively operating on 3,126 online

[16] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/.
[17] https://oag.ca.gov/system/files/US%20Notice%20Proof.pdf.

shops" hosted on Volusion's e-commerce platform.[18]

27. By March 12, 2020, the Gemini Advisory firm identified over 239,000 compromised credit card records from the Data Breach that were sold on the dark web for $1.6 million. Of these 239,000 stolen records, first posted on the dark web in November 2019, 98.97% were for U.S.-issued cards. Gemini estimates that, based on the number of affected merchants, the total number of compromised financial records could be as high as 20 million. At the same cost for which the original set of 239,000 stolen records were sold, the haul could net the hackers as much as $133.89 million on the dark web.[19]

28. Public reporting has linked the Data Breach to "Magecart Group 6," a loose affiliation of cybercriminals known for use of such web skimmers. Magecart Group 6 "is known to only target top-tier victims, investing in scams where they can receive a big payoff from one attack." Previous entities targeted by Magecart Group 6 include British Airways and Newegg.[20]

29. By on or about October 10, 2019, Volusion had removed the malicious source code that compromised its payment processing software. [21]

30. As a result of the Data Breach, Magecart and/or other unauthorized third parties were able to obtain PII from users who had entered their PII when making a purchase through an online store hosted on Volusion's e-commerce platform from on or about October 7, 2019 to on or about October 15, 2019.

31. Specifically, the PII (described above in Paragraph 3) of Plaintiffs and the Class was compromised in the Data Breach.

---

[18] https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.

[19] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/.

[20] https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.

[21] https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/. Volusion claims the malicious code had been removed by October 8, 2019.

32. On or about April 21, 2020 – at least six months *after* Volusion was aware of the Data Breach – Volusion provided notice to Plaintiffs and the Class regarding the data breach through a Notification Letter (which was transmitted via e-mail).[22] The Notification Letter described the Data Breach and the PII that was stolen. It further noted that Volusion had "updated its internal procedures . . . and added additional safeguards to minimize the chance that an incident like this could occur in the future."

33. Volusion did not offer victims of the Data Breach any financial fraud or identity protection services. Such services are often offered by companies that have been the subject of a data breach.[23] The Notification Letter nonetheless instructed Plaintiffs and the Class to "carefully review your payment card account statements, and if you find any suspicious activity report it to the financial institution that issued the account."

34. Web skimming data breaches, like this one, are usually made possible through a vulnerability in a website or its backend content management system.

35. Web skimming is not a new threat. Numerous other similar data breaches establish that Volusion was aware of this threat and did not take sufficient actions to guard against it.

36. For example, in June 2018, major e-commerce vendor Ticketmaster announced it had been the target of a card-skimmer attack by Magecart affecting tens of thousands of customers.[24] Ticketmaster was but one victim of a wide-ranging campaign that targeted

[22] A copy of the Notification Letter received by the Class is available at https://oag.ca.gov/system/files/US%20Notice%20Proof.pdf. A copy of the specific email Notification Letter received by Plaintiff Lopez is attached as **Exhibit A**. A copy of the specific email Notification Letter received by Plaintiff Oros is attached as **Exhibit B**.

[23] *See, e.g.*, https://oag.ca.gov/system/files/GE%20-%20Canon%20HOME%20Letter%2003202020.pdf (offering identity protection and credit monitoring services for two years at no cost).

[24] *See* Tara Seals, *Ticketmaster Chat Feature Leads to Credit-Card Breach* (June 28, 2018), https://threatpost.com/ticketmaster-chat-feature-leads-to-credit-card-breach/133191/.

approximately 800 e-commerce sites.[25]

37. In November 2018, another major e-commerce company, VisionDirect announced that it, too, was the target of a card-skimmer attack by Magecart.[26]

38. In May 2019, RiskIQ announced at least seven different web-based suppliers were targeted in supply-chain attacks involving Magecart web-skimmers.[27]

39. In August 2019, Visa sounded the alarm with a public security alert that warned of "JavaScript skimming attacks against eCommerce service providers," in which "the attackers inject malicious JavaScript code into the websites of merchants and service providers to harvest payment information, such as billing address, account number, expiration date, and CVV2 from the checkout forms on eCommerce pages."[28] This is exactly what happened in the Data Breach.

40. Indeed, on August 1, 2019, PCI Security Standards Council, the organization that administers the Payment Card Industry Data Security Standard ("PCI DDS") to which Volusion claims to adhere, issued a threat bulletin to "highlight an emerging threat that requires urgent awareness and attention": web-skimming attacks by Magecart that "infect e-commerce websites with malicious code, known as *sniffers or JavaScript (JS) sniffers*."[29] The bulletin details several detection and prevention best practices, in accordance with the PCI DDS, which if complied with could have allowed Volusion to protect against the Data Breach or detect it early enough to prevent such wide-spread harm.

41. Volusion did not take the threat seriously, and it did not follow these best practices

---

[25] *See* Tara Seals, *Ticketmaster Breach: Just One Part of a Wide-Ranging Campaign* (July 11, 2018), https://threatpost.com/ticketmaster-breach-just-one-part-of-a-wide-ranging-campaign/133892/.

[26] *See* Lindsey O'Donnel, *VisionDirect Blindsided by Magecart in Data Breach* (November 19, 2019), https://threatpost.com/visiondirect-blindsided-by-magecart-in-data-breach/139223/.

[27] *See* Yonathan Klijnsma, *Magecart Supply-chain Frenzy Continues With AppLixir, RYVIU, OmniKick, eGain, AdMaxim, CloudCMS & Picreel* (May 14, 2019), https://www.riskiq.com/blog/labs/cloudcms-picreel-magecart/.

[28] *Visa Security Alert: eCommerce JavaScript Skimming Campaign Targeting Service Providers*, Visa (August 2019), https://usa.visa.com/dam/VCOM/global/support-legal/documents/java-script-skimming-attacks.pdf.

[29] *The Threat of Online Skimming to Payment Security*, PCI Security Standards Council (August 1, 2019),

and industry standards. If it had, Volusion would have not suffered such a massive Data Breach.

42. Colin Bastable, CEO of Lucy Security, in a statement made to Threatpost shortly after the Volusion Data Breach after yet another company, Macy's, was hit with a card skimmer, observed: "MageCart is not a mystery, by now, one might think that 'additional security measures' would be added to all websites as a matter of course, before hackers drop in some malicious code," adding: "That is the definition of a precaution."[30]

43. At all relevant times, Volusion was well aware, or reasonably should have been aware, that the PII collected, maintained, and stored on its servers is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, fraud and other misuse.

44. Notwithstanding its prior knowledge of the risk of a web skimmer attack, Volusion did not take adequate security measures to protect Plaintiffs' and class members' PII.

Volusion Failed to Comply with Regulatory Guidance and Meet Consumers' Expectations

45. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for

[30] *See* Lindsey O'Donnell, *Macy's Suffers Data Breach by Magecart Cybercriminals* (Nov. 19, 2019), https://threatpost.com/macys-data-breachlinked-to-magecart/150393/.

[31] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 15, 2020).

business.[32] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[33]

47. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[34]

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[35]

49. In this case, Volusion was fully aware of its obligation to use reasonable measures to protect the PII of its users, acknowledging as much in its own Privacy Policy. Volusion also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Volusion failed to comply with industry-standard data security requirements.

---

[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[33] *Id.*
[34] FTC, *Start With Security*, *supra* note 27.
[35] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 15, 2020).

50. Volusion's failure to employ reasonable and appropriate measures to protect against unauthorized access to its users' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 and various state consumer protection and data breach statutes.

Effect of the Data Breach on Impacted Customers

51. Volusion's failure to keep Plaintiffs' and class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach, cyber criminals have the ability to commit identity theft and other identity-related fraud against Plaintiffs and class members now and into the indefinite future.

52. The PII exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years to come. Identity thieves can use the PII to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or medical treatment; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

53. PII has significant monetary value in part because criminals continue their efforts to obtain this data.[36] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17% increase from the total

[36] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE (Sept. 28, 2014), available at http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

number of breaches reported in 2018.[37]

54. The PII of consumers remains of high value to identity criminals, not only through their own direct use of such PII, but also as evidenced by the prices criminals will pay through black-market sources on the dark web. Numerous sources cite dark web pricing for stolen identity credentials, quantifying the loss to victims based on the value of the data itself. For example, a single user's credit card data can fetch $12 on the dark web and bank credentials can fetch over $1,000.[38] Indeed, 239,000 compromised credit card records from the Data Breach that were sold on the dark web for $1.6 million – an average of $6.69 per record (presumably, a bulk discount).

55. Just as companies like Volusion trade on the value of consumers' PII, consumers recognize the value of their PII and offer it in exchange for goods and services. Plaintiffs and the Class gave Volusion their PII in exchange for Volusion's services; namely, the ability to purchase items through online shops hosted on Volusion's e-commerce platform. Further, the value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

56. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[39]

57. The annual cost of identity theft is even higher. McAfee and the Center for Strategic

---

[37] Identity Theft Center, *2019 End-of-Year Data Breach Report* (2019), available at https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

[38] *Here's How Much Thieves Make By Selling Your Personal Data Online,* BUSINESS INSIDER (May 27, 2015), available at http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.

[39] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited July 15, 2020).

and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[40]

58. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[41]

59. Plaintiff Lopez himself already suffered from financial fraud; the same Citibank credit card he used to make a purchase from an online shop hosted on Volusion's e-commerce platform was used to fraudulently purchase a $1,354.09 stay at a luxury hotel and resort on or about January 2, 2020 – after Volusion was aware of the data breach, a little over a month after compromised payment card information from the Data Breach was posted for sale on the dark web, but months before Volusion informed Plaintiff Lopez that his card information had been compromised. Plaintiff Lopez became aware of the fraudulent charge after Citibank sent him a phone alert, and he thereafter spent time disputing the charge and canceling and replacing his credit card; beyond the loss of the productive use of this time, it created annoyance and emotional distress. Plaintiff Lopez's Citibank credit card that was compromised in the Data Breach had never before been compromised in a data breach or otherwise.

60. Even if financial fraud or identity theft has not occurred, consumers may spend valuable time and suffer from the emotional toll of a data breach. Plaintiff Lopez himself has been spending several hours a month monitoring each of his financial accounts since he became the

[40] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited July 15, 2020).
[41] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 15, 2020).

victim of financial fraud as a result of the Data Breach, because although he has canceled his credit card compromised in the breach, he cannot be sure that his card information was not set up by an unauthorized third party in a manner that would allow his account to still be charged (e.g., through recurring payments).[42] He also must now spend time monitoring his credit reports to ensure no other financial accounts or lines of credit are opened in his name. Beyond the loss of productive use of this time, the Data Breach has caused anxiety and otherwise negatively affected Mr. Lopez emotionally.

61. Plaintiff Oros himself already suffered from two fraudulent transactions on his debit card that was compromised in the Data Breach. Mr. Oros was forced to cancel the card and wait for days for a replacement card to arrive. He monitored the account associated with that debit card multiple times a day for months before eventually closing the bank account. Mr. Oros also had to spend a significant amount of time changing the information he had on file with various retailers, vendors, and service providers where he had used that debit card. Since the Data Breach, two people have tried to open accounts in Mr. Oros's name and have attempted to hack his online accounts, and he has been forced to spend extra time monitoring his accounts to try to prevent fraud. Mr. Oros's debit card that was compromised in the Data Breach had never before been compromised in a data breach or otherwise. The Data Breach has also caused anxiety and otherwise negatively impacted Mr. Oros emotionally.

62. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced

[42] https://pocketsense.com/cancel-debit-card-automatic-bills-still-paid-old-card-number-12288.html ("If you cancel a debit card, it is unlikely the merchant will be able to still use the old card number to process a payment. However, in the case of credit cards, merchants can receive a customer's new card information through updater services provided by all four of the major credit card issuers.")

affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[43] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

63. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[44] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.

64. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)

[43] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited July 15, 2020).
[44] *Id.*

- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[45]

65. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[46]

66. The risk of identity theft and financial fraud is particularly acute where detailed personal information is stolen, such as that which was stolen in the Data Breach.

67. Plaintiffs and the Class would not have provided their PII to Volusion if they had known Volusion did not have in place adequate policies and procedures to protect their PII.

68. As the result of the Data Breach, Plaintiffs and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. purchasing goods and services they would not have otherwise paid for and/or paying more for goods and services than they otherwise would have paid, had they known the truth about Defendant's substandard data security practices;

b. losing the inherent value of their PII;

c. losing the value of Volusion's explicit and implicit promises of adequate data security;

d. identity theft and fraud resulting from theft of their PII;

e. costs associated with the detection and prevention of identity theft, financial fraud, and

[45] *Id.*

[46] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited July 15, 2020).

unauthorized use of their online accounts, including financial accounts;

f. costs associated with purchasing credit monitoring and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial account funds, and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties.

69. Additionally, Plaintiffs and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal

information to organizations that suffered a data breach.[47]

70. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Volusion would have no reason to tout their data security efforts to their actual and potential customers.

71. Consequently, had consumers including Plaintiffs known the truth about Volusion's data security practices—that Volusion would not adequately protect and store their data—they would not have entrusted their PII to Volusion and would not have been willing to pay for, or pay as much for, any purchases through online shops hosted on Volusion's e-commerce platform. As such, Plaintiffs and class members did not receive the benefit of their bargain with Volusion because they paid for a value of services, either through PII or a combination of their PII and money, they expected but did not receive.

CLASS ACTION ALLEGATIONS

72. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2) and (b)(3), as applicable, Plaintiffs seek certification of the following nationwide class (the "Nationwide Class"):

73. Nationwide Class: **All persons in the United States whose PII was compromised in the Data Breach.**

74. The Nationwide Class asserts claims against Volusion for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), declaratory judgment (Count 4), and violation of the Texas Deceptive Trade Practices-Consumer Protection Act (Count 5).

75. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2) and (b)(3), as applicable, Plaintiff Lopez seeks certification of Florida state claims in the alternative to the nationwide claims (except for Count 5), as well as statutory claims under Florida's Deceptive and Unfair Trade Practices Act

[47] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited July 15, 2020).

(Count 6) (the "Florida Subclass"), defined as follows:

76. Florida Subclass: **All persons in Florida whose PII was compromised in the Data Breach.**

77. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2) and (b)(3), as applicable, Plaintiff Oros seeks certification of Illinois state claims in the alternative to the nationwide claims (except for Count 5), as well as statutory claims under the Illinois Personal Information Protection Act (Count 7), Illinois Consumer Fraud Act (Count 8), and Illinois Uniform Deceptive Trade Practices Act (Count 9) (the "Illinois Subclass"), defined as follows:

78. Illinois Subclass: **All persons in Illinois whose PII was compromised in the Data Breach.**

79. Excluded from the Nationwide Class and the Florida and Illinois Subclasses[48] are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and the Florida and Illinois Subclasses are any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

80. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

81. Each of the proposed classes meets the criteria for certification under Rule 23(a), (b)(1), (b)(2), (b)(3) and (c)(4).

82. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed class members include thousands of consumers across all 50 states, there is significant risk of inconsistent or varying adjudications with respect to individual class members that would

[48] The Nationwide Class, the Florida Subclass, and the Illinois Subclass are sometimes referred to collectively herein as "the Class."

establish incompatible standards of conduct for the Defendant. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing the Defendant to have to choose between differing means of upgrading their data security infrastructure and choosing the court order with which it will comply.

83. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Nationwide Class and the Florida and Illinois Subclasses are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiff at this time, public researchers have identified 239,000 compromised records that were already sold on the dark web. This suggests the Class includes, at minimum, hundreds of thousands of members and indeed, likely millions based on the number of merchant clients' stores affected by the Data Breach, as described above. Affected consumer's names, e-mail addresses, and physical addresses are available from Volusion's records, and class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice.

84. **Predominance of Common Issues. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include:

a. Whether Defendant knew or should have known that its computer and data storage systems, including payment processing software and systems, were vulnerable to attack;

b. Whether Defendant omitted or misrepresented material facts regarding the security of its computer and data storage systems and its inability to protect vast amounts of consumer data, including Plaintiffs' and class members' PII;

c. Whether Defendant failed to take adequate and reasonable measures to ensure such

computer and data systems were protected;

d. Whether Defendant failed to take available steps to prevent and stop the Data Breach from happening;

e. Whether Defendant owed duties to Plaintiffs and class members to protect their PII;

f. Whether Defendant owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

g. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

h. Whether Defendant breached its duties to protect the PII of Plaintiffs and class members by failing to provide adequate data security;

i. Whether Defendant's failure to secure Plaintiffs' and class members' PII in the manner alleged violated federal, state and local laws, or industry standards;

j. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and class members' PII;

k. Whether Defendant's conduct amounted to violations of state consumer protection statutes;

l. Whether, as a result of Defendant's conduct, Plaintiffs and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

m. Whether, as a result of Defendant's conduct, Plaintiffs and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

85. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to the Nationwide Class and the Florida and Illinois Subclasses, Plaintiffs' claims are typical of other class members' claims because Plaintiffs

and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

86. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff Lopez is an adequate representative of the Nationwide Class and the Florida Subclass because Plaintiff Lopez is a member of the Nationwide Class and the Florida Subclass, and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff Oros is an adequate representative of the Nationwide Class and the Illinois Subclass because Plaintiff Oros is a member of the Nationwide Class and the Illinois Subclass, and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of the Nationwide Class and the Florida and Illinois Subclasses.

87. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer

management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

88. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2) and (c).** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Nationwide Class and the Florida and Illinois Subclasses as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retains possession of at least some of Plaintiffs' and the class members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

89. All members of the proposed Class are readily ascertainable. Volusion has access to information regarding which individuals were affected by the Data Breach, as evidenced by the Notification Letter it sent to Plaintiffs and class members. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

Count 1

NEGLIGENCE

Against Volusion on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Florida and Illinois Subclasses

90. Plaintiffs repeat the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein.

91. Volusion required Plaintiffs and class members to submit sensitive PII in order to purchase goods through online shops hosted on Volusion's e-commerce platform. Volusion stored

this vast treasure trove of PII on its computer systems.

92. By collecting, storing, using, and profiting from this data, Volusion had a duty of care to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's security systems, data storage architecture, and payment processing software to ensure that Plaintiffs' and class members' PII was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Defendant's security systems, data storage architecture, and payment processing software in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Defendant's security vulnerabilities and potential compromise of the PII of Plaintiffs and class members; (d) maintaining data security measures consistent with industry standards; and (e) timely and adequately informing class members if and when a data breach occurred notwithstanding undertaking (a) through (d) above.

93. Volusion had common law duties to prevent foreseeable harm to Plaintiffs and class members. These duties existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and other class members would be harmed by such theft.

94. Defendant had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected, stored, and processed by Volusion's computer systems and payment software.

95. Defendant's duties to use reasonable security measures also arose as a result of the

special relationship that existed between Defendant, on the one hand, and Plaintiffs and class members, on the other hand. The special relationship arose because Plaintiffs and class members entrusted Defendant with their PII as part of process for purchasing items through online shops hosted on Volusion's e-commerce platform. Defendant alone could have ensured that its security systems, data storage architecture, and payment processing software were sufficient to prevent or minimize the Data Breach.

96. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

97. Defendant knew or should have known that its computer systems, data storage architecture, and payment processing software were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

98. Defendant breached the duties it owed to Plaintiffs and class members described above and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) timely notify Plaintiffs and class members of the Data Breach.

99. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and class members, their PII would not have been compromised.

100. As a direct and proximate result of Defendant's negligence, Plaintiffs and class

members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, payment card statements, and credit reports and replacing payment cards; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 2

NEGLIGENCE *PER SE*

Against Volusion on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Florida and Illinois Subclasses

101. Plaintiffs repeat the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein.

102. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

103. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and

the foreseeable consequences of a data breach on Defendant's systems.

104. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

105. Plaintiffs and class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

106. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and class members.

107. As a direct and proximate result of Defendant's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, payment card statements, and credit reports and replacing payment cards; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 3

UNJUST ENRICHMENT

Against Volusion on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Florida and Illinois Subclasses

108. Plaintiffs repeat the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein and plead this claim, to the extent necessary, in the alternative to their claims at law.

109. Plaintiffs and class members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Data Breach.

110. Defendant was benefited by the conferral upon it of the PII pertaining to Plaintiffs and class members and by its ability to retain, use, and profit from that information. Defendant understood that it was in fact so benefited.

111. Defendant also understood and appreciated that the PII pertaining to Plaintiffs and class members was private and confidential and its value depended upon Defendant's maintaining the privacy and confidentiality of that PII.

112. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant.

113. Defendant continues to benefit and profit from its retention and use of the PII while its value to Plaintiffs and class members has been diminished. Collecting PII confers a benefit on companies such as Volusion because it allows such companies to analyze customer traffic and enhance and improve their service offerings, as recognized in Volusion's Privacy Policy.

114. Defendant also benefitted through its unjust conduct by its merchant customers being able to sell goods and services through Volusion's e-commerce platform (thus ensuring their financial solvency and ability to continue paying Volusion for use of its e-commerce platform) to

Plaintiffs and class members, who would not have purchased goods or services from online shops hosted on Volusion's e-commerce platform at all, or at the terms offered, had they been aware that Defendant would fail to protect their PII.

115. Volusion also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and class members' PII.

116. It is inequitable for Defendant to retain these benefits.

117. As a result of Defendant's wrongful conduct as alleged in this Complaint (including, among other conduct, its knowing failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and class members without having adequate data security measures, and its other conduct facilitating the theft of that PII), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members.

118. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and class members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

119. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and class members in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

120. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

121. Plaintiffs and class members have no adequate remedy at law.

122. Defendant is therefore liable to Plaintiffs and class members for restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically: the value to Defendant of the PII that was stolen in the Data Breach; the profits Defendant is receiving from the use of that information; the amount that Volusion's merchant customers overcharged Plaintiffs and class members for goods and services purchased from online shops hosted on the Volusion e-commerce platform; and the amounts that Volusion should have spent to provide reasonable and adequate data security to protect Plaintiffs' and class members' PII.

Count 4

DECLARATORY JUDGMENT

Against Volusion on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Florida and Illinois Subclasses

123. Plaintiffs repeat the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein

124. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

125. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its merchant clients' customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their PII. Plaintiffs and class members remain at imminent risk that further

compromises of their PII will occur in the future. This is true even if they are not actively using Defendant's website.

126. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

127. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

128. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Volusion. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

129. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Volusion, Plaintiffs and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

130. Issuance of the requested injunction will not disserve the public interest. To the

contrary, such an injunction would benefit the public by preventing another data breach at Volusion, thus eliminating additional injuries that would result to Plaintiffs, class members, and the millions of consumers whose PII would be further compromised.

Count 5

TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT,

Texas Bus. & Com. Code §§ 17.41, et seq.

Against Volusion on Behalf of Plaintiffs and the Nationwide Class

131. Plaintiffs repeat the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein.

132. Defendant is a "person" as defined by Tex. Bus. & Com. Code § 17.45(3).

133. Plaintiffs and the class members are "consumer[s]" as defined by Tex. Bus. & Com. Code § 17.45(4)

134. Defendant engaged in trade or commerce as defined by Tex. Bus. & Com. Code § 17.45(6).

135. Defendant engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Failing to disclose information concerning goods or services which was known at the time of the transaction where such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have

entered had the information been disclosed.

136. Defendant's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Nationwide Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and the Nationwide Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the Nationwide Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Nationwide Class members' PII, including duties imposed by the FTC Act, 15

U.S.C. § 45.

137. For its misrepresentations, those were ongoing misrepresentations made by Volusion through its Privacy Policy to Volusion's merchant clients, and Volusion also omitted material information. Had Volusion made appropriate disclosures – e.g., on the payment processing pages that were compromised, Plaintiffs and class members would not have purchased products on webpages using Volusion's payment processing software or would have paid less for such products.

138. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers and Volusion's merchant clients about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' PII.

139. Had Defendant disclosed to Plaintiffs and class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and class members' PII as part of the services the Defendant provided and for which Plaintiffs and class members paid through their purchase of goods and services at online shops hosted on Volusion's e-commerce platform without advising Plaintiffs and class members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and class members' PII. Accordingly, Plaintiffs and the Nationwide Class members, and Volusion's merchant clients, acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

140. Defendant had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the PII in its possession. This duty arose because Plaintiffs and the Nationwide Class members reposed a trust and confidence in the Defendant when they provided their PII to the Defendant in exchange for the ability to purchase goods and services from

online shops hosted on Volusion's e-commerce platform. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Nationwide Class members, and Defendant because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the PII;

b. Active concealment of the state of its data security measures and systems;

c. Incomplete representations about the security and integrity of its computer and data storage systems, including payment processing software, while purposefully withholding material facts from its merchant clients, Plaintiffs, and the Nationwide Class members that contradicted these representations and omissions.

141. Defendant engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendant engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree. Defendant's unconscionable actions include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Nationwide Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties

imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and the Nationwide Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the Nationwide Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Nationwide Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

142. Consumers, including Plaintiffs and the Nationwide Class members, lacked knowledge about deficiencies in Defendant's data security because this information was known exclusively by the Defendant. Consumers also lacked the ability, experience, or capacity to secure the PII in Defendant's possession or to fully protect their interests with regard to their data. Plaintiffs and the Nationwide Class members lack expertise in information security matters and do not have access to the Defendant's systems in order to evaluate its security controls. Defendant took advantage of its special skill and access to the PII to hide its inability to protect the security and confidentiality of Plaintiffs' and the Nationwide Class members' PII.

143. Defendant intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that

would result. The unfairness resulting from Defendant's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Defendant's false, misleading, deceptive, and unconscionable business acts and practices, exposed Plaintiffs and the Nationwide Class members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and the Nationwide Class members cannot mitigate this unfairness because they cannot undo the Data Breach.

144. Defendant acted knowingly and maliciously to violate Texas's Deceptive Trade Practices—Consumer Protection Act, and recklessly disregarded Plaintiffs' and the Nationwide Class members' rights. Defendant is of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put it on notice that its security and privacy protections were inadequate.

145. As a direct and proximate result of Defendant's false, misleading, deceptive, and unconscionable acts and practices, Plaintiffs and the Nationwide Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, payment card statements, and credit reports and replacing payment cards; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and

other economic and non-economic harm.

146. The Defendant's deceptive, unfair, and unconscionable acts and practices complained of herein affected the public interest and consumers at large, including the hundreds of thousands, if not millions, of Nationwide Class members affected by the Data Breach.

147. Defendant's unconscionable, unfair, and deceptive acts or practices were a producing cause of Plaintiffs' and the Nationwide Class members' injuries, ascertainable losses, and economic and non-economic damages.

148. The Defendant's violation presents a continuing risk to Plaintiffs and the Nationwide Class members as well as to the general public.

149. Plaintiffs and the Nationwide Class members seek injunctive relief, other equitable relief the court deems proper, and reasonable and necessary attorneys' fees. As Plaintiffs have provided Defendant sixty days written notice of this claim, they are also seeking compensatory damages including mental anguish damages and economic damages, and also statutory additional damages in the amount of three times the economic and mental anguish damages, as Defendant's actions were knowing.

Count 6

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201, et seq.

Against Volusion on Behalf of Plaintiff Lopez and the Florida Subclass

150. Plaintiff Lopez repeats the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein.

151. Plaintiff Lopez and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

152. Volusion advertised, offered, or sold goods or services in Florida and engaged in

trade or commerce directly or indirectly affecting the people of Florida.

153. Volusion engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, or to remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Florida Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Florida Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs'

and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. § 501.171(2).

154. For its misrepresentations, those were ongoing misrepresentations made by Volusion through its Privacy Policy to Volusion's merchant clients, Plaintiff Lopez, and class members. For its omissions, those were omissions made by Volusion that were ongoing and targeted at Plaintiff Lopez, class members, and Volusion's merchant clients.

155. Volusion's representations and omissions were material because they were likely to deceive reasonable consumers, as well as Volusion's merchant clients, about the adequacy of Volusion's data security and ability to protect the confidentiality of consumers' PII.

156. Volusion intended to mislead Plaintiff Lopez and Florida Subclass members, as well as its merchant clients, and induce them to rely on its misrepresentations and omissions.

157. Had Volusion disclosed to Plaintiff Lopez and Florida Subclass members, or to its merchant clients, that its data systems were not secure and, thus, vulnerable to attack, Volusion would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Volusion received, maintained, and compiled Plaintiff Lopez's and Florida Subclass members' PII as part of the services Volusion provided and for which Plaintiff Lopez and Florida Subclass members paid without advising Plaintiff Lopez and Florida Subclass members that Volusion's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff Lopez's and Florida Subclass members' PII. Accordingly, Plaintiff Lopez and the Florida Subclass members, as well as Volusion's merchant clients, acted reasonably in relying on Volusion's misrepresentations and omissions, the truth of which they could not have discovered.

158. Volusion acted knowingly and maliciously to violate the Florida Deceptive and Unfair Trade Practices Act, and recklessly disregarded Plaintiff Lopez's and Florida Subclass

members' rights. Past breaches within the e-commerce industry, including by the same hacker group Magecart, put Volusion on notice that its security and privacy protections were inadequate.

159. As a direct and proximate result of Volusion's unfair, unconscionable, and deceptive acts and practices, Plaintiff Lopez and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, payment card statements, and credit reports and replacing payment cards; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

160. Plaintiff Lopez and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

Count 7

ILLINOIS PERSONAL INFORMATION PROTECTION ACT

815 ILCS 530/10(a), et seq.

Against Volusion on Behalf of Plaintiff Oros and the Illinois Subclass

161. Plaintiff Oros repeats the allegations in paragraphs 1 – 89 in this Complaint, as if

fully alleged herein.

162. Defendant is a "data collector" as defined by 85 ILCS 530/5.

163. Plaintiff Oros and the Illinois Subclass members' PII includes "personal information" as covered under 815 ILCS 530/5.

164. As a data collector, Defendant is required to notify Plaintiff Oros and the Illinois Subclass members of a data breach in its data security systems in the most expedient time possible and without unreasonable delay pursuant to 815 ILCS 530/10(a).

165. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Defendant violated 815 ILCS 530/10(a).

166. Pursuant to 815 ILCS 530/20, a violation of 815 ILCS 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

167. As a direct and proximate result of Defendant's violation of 815 ILCS 530/10(a), Plaintiff Oros and Illinois Subclass members suffered damages, as described above.

168. Plaintiff Oros and Illinois Subclass member seek relief under 815 ILCS 510/3 for the harm they suffered because of Defendant's willful violations of 815 ILCS 530/10(a), including actual damages, equitable relief, and attorneys' fees.

Count 8

ILLINOIS CONSUMER FRAUD ACT

815 ILCS 505, et seq.

Against Volusion on Behalf of Plaintiff Oros and the Illinois Subclass

169. Plaintiff Oros repeats the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein.

170. Defendant is a "person" as defined by 815 ILCS 505/1(c).

171. Plaintiff Oros and Illinois Subclass members are "consumers" as defined by 815

ILCS 505/1(e).

172. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS 505/1(f).

173. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 ILCS 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, or to remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Personal Information Protection Act, 815 ILCS 530/10(a), and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Personal Information Protection Act, 815 ILCS 530/10(a), and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2(a).

174. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and the ability to protect the confidentiality of consumers' PII.

175. Defendant intended to mislead Plaintiff Oros and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

176. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid, and that injury outweighed any countervailing benefits to consumers or competition.

177. Defendant acted knowingly and maliciously to violate the Illinois Consumer Fraud Act, and recklessly disregarded Plaintiff Oros and the Illinois Subclass members' rights. Defendant knew or, with the exercise of reasonable care, should have known that its security and privacy protections were inadequate.

178. As a direct and proximate result of Volusion's unfair, unconscionable, and deceptive acts and practices, Plaintiff Oros and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, payment card statements, and credit reports and replacing payment cards; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

179. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

Count 9

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

815 ILCS 510/25, et seq.

Against Volusion on Behalf of Plaintiff Oros and the Illinois Subclass

180. Plaintiff Oros repeats the allegations in paragraphs 1 – 89 in this Complaint, as if fully alleged herein.

181. Defendant is a "person" as defined by 815 ILCS 510/1(5).

182. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS 510/2(a).

183. Defendant's deceptive trade practices include:

h. Failing to implement and maintain reasonable security and privacy measures to

protect Plaintiff's and Illinois Subclass members' PII, which was a direct and proximate cause of the Data Breach;

i. Failing to identify foreseeable security and privacy risks, or to remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

j. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2(a), which was a direct and proximate cause of the Data Breach;

k. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

l. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Personal Information Protection Act, 815 ILCS 530/10(a), and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2(a);

m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass members' PII; and

n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Personal Information Protection Act, 815 ILCS

530/10(a), and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2(a).

184. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and the ability to protect the confidentiality of consumers' PII.

185. Defendant intended to mislead Plaintiff Oros and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

186. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid, and that injury outweighed any countervailing benefits to consumers or competition.

187. Defendant acted knowingly and maliciously to violate the Illinois Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Oros and the Illinois Subclass members' rights. Defendant knew or, with the exercise of reasonable care, should have known that its security and privacy protections were inadequate.

188. As a direct and proximate result of Volusion's unfair, unconscionable, and deceptive acts and practices, Plaintiff Oros and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach

reviewing bank statements, payment card statements, and credit reports and replacing payment cards; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

189. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

1) For an Order certifying the Nationwide Class and the Florida and Illinois Subclasses, as defined herein, and appointing Plaintiffs and Plaintiffs' counsel to represent the Class as alleged herein;
2) For injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:
    a) Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
    b) Requiring Defendant to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
    c) Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and class members unless Volusion can provide the Court a reasonable justification for the retention and use of such information when weighed against the privacy interests of

Plaintiffs and the class members;

d) Requiring Volusion to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and class members' PII;

e) Requiring Volusion to engage independent third-party security auditors and internal personnel to run automated security monitoring;

f) Requiring Volusion to audit, test, and train their security personnel regarding any new or modified procedures;

g) Requiring Volusion to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h) Requiring Defendant to conduct regular database scanning and security checks;

i) Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and class members;

j) Requiring Defendant to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

k) Requiring Defendant to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor the Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l) Requiring Defendant to meaningfully educate all class members about the threats they

face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

m) Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

n) Requiring Defendant to provide identity protection and financial fraud monitoring services at no cost to Plaintiffs and the class members;

3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

4) For an award of statutory damages, trebled, and punitive or exemplary damages, as allowed by law in an amount to be determined;

5) For an award of restitution or disgorgement, in an amount to be determined;

6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: July 17, 2020

Respectfully submitted,

/s/ Michael Singley
Jeff Edwards
Tex. Bar No. 24014406
Michael Singley
Tex. Bar No. 00794642
David James
Tex. Bar No. 24092572
EDWARDS LAW GROUP
1101 East 11th St.
Austin, TX 78702
512-623-7727
Fax: 512-623-7729
mike@edwards-law.com
jeff@edwards-law.com
david@edwards-law.com

Jeff Ostrow*
Fla. Bar No. 121452
Jonathan M. Streisfeld*
Fla. Bar No. 117447
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
1 West Las Olas Blvd. Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Facsimile: (954) 525-4300
Email: streisfeld@kolawyers.com
ostrow@kolawyers.com

Hassan A. Zavareei*
Cal. Bar No. 181547
D.C. Bar. No. 456161
Mark A. Clifford*
D.C. Bar. No. 155088
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
Email: hzavareei@tzlegal.com
mclifford@tzlegal.com

Melissa S. Weiner*
MN Bar No. 0387900
Joseph C. Bourne*
MN Bar No. 0389922
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610
Email: mweiner@pswlaw.com
jbourne@pswlaw.com

**pro hac vice* application forthcoming

Counsel for Plaintiffs and the Proposed Class